KRIPTOSISTEM GABUNGAN S-ECIES DAN RSA

Tamado Ramot Sitohang, Rini Marwati, Isnie Yusnitha

Departemen Pendidikan Matematika FPMIPA UPI

*Surel: tamado.sitohang@gmail.com

ABSTRAK. Keamanan data merupakan aspek yang sangat penting pada era teknologi informasi. Transmisi data yang tidak aman dapat menyebabkan kerugian yang besar. Untuk mengatasi masalah tersebut, diperlukan ilmu kriptografi. Ilmu kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan dan keaslian data, autentikasi entitas, dan autentikasi sumber data. Contoh-contoh algoritma kriptografi yang sering digunakan saat ini adalah *Elliptic Curve Cryptography* dan RSA. *Elliptic Curve Cryptography* menggunakan grup siklik pada himpunan titik pada kurva eliptik di bawah operasi penjumlahan titik untuk melakukan operasi-operasi kriptografi. Salah satu kriptosistem yang termasuk ke dalam *Elliptic Curve Cryptography* adalah *Simplified Elliptic Curve Integrated Encryption Scheme*. Kriptosistem RSA adalah kriptosistem yang didasarkan pada sulitnya memfaktorkan sebuah bilangan menjadi dua buah bilangan prima yang berbeda. Dalam penelitian ini akan disajikan pengembangan kriptosistem *Simplified Elliptic Curve Integrated Encryption Scheme* dan RSA dengan cara menggabungkannya. Penggabungan kedua kriptosistem tersebut bertujuan untuk mempersulit kriptanalis untuk memecahkan ciphertext.

Kata Kunci: *Elliptic Curve Cryptography*, *Simplified Elliptic Curve Integrated Encryption Scheme*, Kriptosistem RSA

ABSTRACT. Data security is a very important aspect in the era of information technology. Unsecured data transmission may cause big losses. Cryptography is needed to solve this problem. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Examples of widely used cryptographic algorithm nowadays is Elliptic Curve Cryptography and RSA. Elliptic Curve Cryptography uses the cyclic group on the set of points in elliptic curve under operation of point addition to do cryptographic operations. One cryptosystem which is classified into Elliptic Curve Cryptography is Simplified Elliptic Curve

Integrated Encryption Scheme. RSA cryptosystem is a cryptosystem which is based on the difficulty of factoring a number into two different prime numbers. This research presents the development of Simplified Elliptic Curve Integrated Encryption Scheme and RSA cryptosystem by combining them and implementing the result into a computer program. Combinating those two cryptosystem aims to complicate cryptanalyst to solve the ciphertext.

Keywords: Elliptic Curve Cryptography, Simplified Elliptic Curve Integrated Encryption Scheme, RSA Cryptosystem

1. PENDAHULUAN

Di era teknologi informasi seperti sekarang ini, masalah keamanan data merupakan aspek yang sangat penting, baik bagi individu, perusahaan maupun negara. Bagi negara, aspek kemanan data ini, terutama dalam transmisi data, menjadi kunci kesuksesan dan kekuatan militer negara tersebut, terutama dalam perang. Transmisi data yang tidak aman dapat menyebabkan data tersebut jatuh ke tangan musuh yang berakibat fatal dan dapat mengubah jalannya perang. Bagi perusahaan, keamanan data menjadi penting dikarenakan banyak data perusahaan yang sifatnya rahasia. Apabila data rahasia ini jatuh ke tangan kompetitor, perusahaan dapat mengalami kerugian yang besar.

Untuk mengatasi masalah-masalah terkait keamanan data, diperlukan ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan dan keaslian data, autentikasi entitas, dan autentikasi sumber data [3].

Algoritma kriptografi terbagi menjadi algoritma kriptografi simetris dan algoritma kriptografi asimetris atau kriptografi kunci publik. Algoritma kriptografi simetris adalah algoritma kriptografi yang kunci dekripsinya dapat diperoleh dengan mudah dari kunci enkripsinya, sedangkan algoritma kriptografi asimetris atau algoritma kriptografi kunci publik adalah algoritma kriptografi yang menggunakan dua kunci yang berbeda dalam proses enkripsi dan dekripsi [1]. Saat ini, algoritma kriptografi asimetris yang banyak digunakan adalah algoritma kriptosistem RSA, algoritma kriptosistem ElGamal, dan algoritma-algoritma kriptografi *Elliptic Curve* (ECC) yang menggunakan kurva eliptik seperti *Elliptic Curve Integrated Encryption Scheme* (ECIES), Simplified Elliptic Curve Integrated Encryption Scheme (S-ECIES) dan ECC ElGamal.

Kriptosistem RSA terkenal keamanannya karena masalah pemfaktoran bilangan bulat. Keamanan kriptosistem RSA dapat ditingkatkan dengan menggunakan tiga bilangan prima pada pembangkitan kuncinya [6]. Sedangkan

ECC terkenal keamanannya karena masalah Elliptic Curve Discrete Logarithm Problem (ECDLP). Oleh karena itu, dalam penelitan ini, dilakukan pengembangan dua kriptosistem tersebut agar diperoleh suatu kriptosistem baru yaitu dengan menggabungkan S-ECIES dan RSA.

2. KURVA ELIPTIK

Kurva eliptik didefinisikan sebagai berikut [2]: Diberikan $a, b \in \mathbb{R}$ sedemikian sehingga $4a^3 + 27b^2 \neq 0$. Sebuah kurva eliptik E adalah himpunan solusi yang terdiri atas pasangan-pasangan terurut $(x, y) \in \mathbb{R} \times \mathbb{R}$ yang memenuhi:

$$y^2 = x^3 + ax + b$$

bersama dengan titik khusus $\boldsymbol{\mathcal{O}}$ yang disebut **titik infinity**.

Kurva eliptik dapat pula didefinisikan pada lapangan berhingga $\mathbb{Z}_p$ sebagai berikut: Diberikan $p > 3$ bilangan prima. Kurva eliptik $y^2 = x^3 + ax + b$ atas $\mathbb{Z}_p$ adalah himpunan solusi E yang terdiri atas pasangan-pasangan terurut $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ yang memenuhi:

$$y^2 \equiv x^3 + ax + b \ (\textbf{mod}\ p)$$

di mana $a, b \in \mathbb{Z}_p$ memenuhi $4a^3 + 27b^2 \not\equiv 0 \ (\textbf{mod}\ p)$, bersama dengan titik khusus $\boldsymbol{\mathcal{O}}$ yang disebut **titik *infinity***.

Kurva eliptik pada lapangan $\mathbb{Z}_p$ membentuk **grup Abelian**, dengan operasi $\oplus$ (penjumlahan titik), yang didefinisikan sebagai berikut:

1. $\boldsymbol{\mathcal{O}}$ merupakan unsur identitas, sehingga $P \oplus \boldsymbol{\mathcal{O}} = \boldsymbol{\mathcal{O}} \oplus P = P$ untuk setiap $P \in E$.
2. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$ dan $Q = (x_1, -y_1)$, maka $P \oplus Q = \boldsymbol{\mathcal{O}}$. Titik Q adalah unsur negatif dari P, dapat ditulis $-P$.
3. Diberikan $P, Q \in E$, di mana $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \neq \boldsymbol{\mathcal{O}}$, $Q \neq \boldsymbol{\mathcal{O}}$, dan $Q \neq \pm P$, maka $P \oplus Q = R = (x_3, y_3)$ di mana:
   $$x_3 = \lambda^2 - x_1 - x_2 \ (\textbf{mod}\ p)$$
   dan
   $$y_3 = \lambda(x_1 - x_3) - x_2 \ (\textbf{mod}\ p)$$
   dengan
   $$\lambda = (-y_3 - y_1)(x_3 - x_1)^{-1}$$
4. Diberikan $P \in E$, di mana $P = (x_1, y_1)$, maka $P \oplus P = 2P = (x_3, y_3)$, disebut juga dengan penggandaan titik, di mana:
   $$x_3 = \lambda^2 - x_1 - x_3 \ (\textbf{mod}\ p)$$
   dan
   $$y_3 = \lambda^2(x_1 - x_3) - x_2 \ (\textbf{mod}\ p)$$

dengan

$$\lambda = (3x_1^2 + a)(2y_1)^{-1} \ (\mathbf{mod}\ p)$$

Selain operasi penjumlahan, pada kurva eliptik pada lapangan $\mathbb{Z}_p$ dapat didefinisikan **multiplikasi titik** dengan aturan:

$$nP = \underbrace{P \oplus P \oplus P \oplus \cdots \oplus P}_{n}$$

dengan $n \in \mathbb{Z}$ dan $P \in E$.

Elliptic Curve Discrete Logarithm Problem adalah sebagai berikut: diberikan sebuah kurva eliptik E atas lapangan berhingga $\mathbb{Z}_p$, sebuah titik $P \in E$ dengan order n dan sebuah titik $Q \in \langle P \rangle$ maka tentukan nilai bilangan bulat $l \in [0, n-1]$ sedemikian sehingga $Q = lP$. Bilangan bulat l disebut ***discrete logarithm* dari Q dengan basis P**, dinotasikan $l = \log_P Q$.

3. KRIPTOSISTEM RSA DAN KRIPTOSISTEM S-ECIES

Menurut Stinson [4], kriptosistem adalah 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, yang memenuhi kondisi-kondisi berikut:

1. $\mathcal{P}$ adalah himpunan berhingga dari *plaintext*
2. $\mathcal{C}$ adalah himpunan berhingga dari *ciphertext*
3. $\mathcal{K}$ adalah *keyspace* yaitu himpunan berhingga dari kunci-kunci
4. Untuk setiap $K \in \mathcal{K}$, terdapat aturan enkripsi $e_K \in \mathcal{E}$ yang berkorespondensi dengan aturan dekripsi $d_K \in \mathcal{D}$. Setiap $e_K : P \to C$ dan $d_K : C \to P$ adalah suatu fungsi sedemikian sehingga $d_K(e_K(x)) = x$ untuk setiap $x \in \mathcal{P}$.

Kriptosistem RSA ditemukan oleh tiga orang peneliti dari Massachusetts Institute of Technology (MIT) yaitu Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1977. Keamanan kriptosistem RSA didasarkan pada tingkat kesulitan untuk memfaktorkan suatu bilangan menjadi dua buah bilangan prima. Untuk memecahkan masalah ini, dibutuhkan algoritma dengan kompleksitas eksponensial. Kriptosistem RSA dapat didefinisikan sebagai berikut [4]: Diberikan $n = pq$, di mana p dan q merupakan bilangan prima. Diberikan $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, didefinisikan:

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \ (\mathbf{mod}\ \phi(n))\}$$

Untuk $K = (n, p, q, a, b)$, didefinisikan:

$$e_K(x) = x^b \ \mathbf{mod}\ n$$

dan

$$d_K(y) = y^a \ \mathbf{mod}\ n$$

dengan $x, y \in \mathbb{Z}_n$. Nilai-nilai n dan b membentuk kunci publik, dan nilai-nilai p, q dan a membentuk kunci privat.

Langkah-langkah pembangkitan kunci adalah sebagai berikut:

1. Bangkitkan dua buah bilangan prima p dan q dengan $p \neq q$
2. Hitung nilai $n = pq$ dan $\phi(n) = (p-1)(q-1)$
3. Pilih bilangan prima acak b, $1 < b < \phi(n)$, sedemikian sehingga $\text{FPB}\big(b, \phi(n)\big) = 1$
4. Hitung nilai $a = b^{-1} \textbf{ mod } \phi(n)$
5. Kunci publik adalah (n, b) dan kunci privat adalah (p, q, a).

Langkah-langkah enkripsi adalah sebagai berikut:

1. Bob mendapatkan kunci publik Alice (n, b)
2. Representasikan pesan sebagai bilangan bulat m pada interval $[0, n-1]$
3. Hitung $y = x^b \textbf{ mod } n$
4. Kirimkan *ciphertext* y kepada Alice

Langkah-langkah dekripsi adalah sebagai berikut:

1. $x \leftarrow y^a \textbf{ mod } n$
2. Ubah bilangan bulat x menjadi *plaintext* sebenarnya

Kriptosistem S-ECIES (*Simplified* ECIES) merupakan simplifikasi dari kriptosistem *Elliptic Curve Integrated Encryption Scheme* (ECIES). S-ECIES termasuk ke dalam *Elliptic Curve Cryptography*, sehingga ECDLP berlaku pada kriptosistem ini. Untuk memecahkan masalah ECDLP, dibutuhkan algoritma dengan kompleksitas eksponensial. S-ECIES mudah diimplementasikan, karena *plaintext* hanya disembunyikan (*masking*) pada titik-titik pada kurva eliptik E. Nilai x dari sebuah titik (x, y) pada kurva eliptik digunakan untuk *masking* sehingga *plaintext* tidak harus berada dalam kurva eliptik E. Susantio dan Muchtadi-Alamsyah [5] mengimplementasikan S-ECIES ke dalam lapangan berhingga *binary field*. Sedangkan pada artikel ini akan digunakan S-ECIES pada lapangan berhingga $\mathbb{Z}_p$.

Kriptosistem S-ECIES menggunakan *point compression* (kompresi titik) untuk meminimalisasi penggunaan memori dalam menyimpan titik pada kurva eliptik yang digunakan. Kompresi titik ini dapat dijabarkan sebagai berikut: Sebuah titik $P \neq \boldsymbol{\mathcal{O}}$ pada kurva eliptik E adalah pasangan terurut (x, y), di mana $y^2 = x^3 + ax + b$ $(\textbf{mod } p)$. Jika diberikan nilai x, terdapat dua nilai y yang mungkin. Kedua nilai tersebut jika dijumlahkan modulo p menghasilkan 0 $(\textbf{mod } p)$. Karena p ganjil, maka salah satu nilai yang mungkin adalah ganjil dan satunya lagi genap. Maka, dapat ditentukan sebuah titik yang unik $P = (x, y) \in E$ hanya dengan mengetahui nilai x dan $y \textbf{ mod } 2$. Nilai $(x, y \textbf{ mod } 2)$ inilah yang merupakan hasil kompresi titik dari (x, y).

Kompresi titik ini dapat mengurangi memori yang digunakan hingga hampir 50%, namun dengan kelemahan harus ditambahkan langkah komputasi untuk merekonstruksi kembali y. Untuk merekonstruksi kembali y, digunakan algoritma yang bergantung pada apakah $x^2 + ax + b$ merupakan *quadratic residue* modulo p. *Quadratic residue* modulo p dapat didefinisikan sebagai berikut: Diberikan p bilangan prima ganjil dan a sebuah bilangan bulat. a merupakan sebuah *quadratic residue* modulo p jika $a \not\equiv 0 \,(\mathbf{mod}\, p)$ dan kongruensi $y^2 \equiv a \,(\mathbf{mod}\, p)$ mempunyai solusi $y \in \mathbb{Z}_p$. a merupakan sebuah *quadratic non-residue* modulo p jika $a \not\equiv 0 \,(\mathbf{mod}\, p)$ dan a bukan *quadratic residue* modulo p jika $a \equiv 0 \,(\mathbf{mod}\, p)(?)$. Kami merancang operasi dekompresi titik yang digunakan untuk merekonstruksi $P = (x, y) \in E$ dari $(x, y \,\mathbf{mod}\, 2)$, dapat diimplementasikan sebagai algoritma berikut.

PROGRAM POINT-DECOMPRESS(x, i)
INPUT: (x, i)
OUTPUT: $P = (x, y) \in E$

$z \leftarrow x^3 + ax + b \,\mathbf{mod}\, p$
if z adalah sebuah *quadratic non-residue* modulo p **then return** "Gagal"
else
    $y \leftarrow \sqrt{z} \,\mathbf{mod}\, p$
    if $y \equiv i \,\mathbf{mod}\, 2$ **then return** (x, y)
    else return $(x, p - y)$

Kriptosistem S-ECIES didefinisikan sebagai berikut [4]. Diberikan E sebuah kurva eliptik pada lapangan $\mathbb{Z}_p$ ($p > 3$ bilangan prima) sedemikian sehingga terdapat $H = \langle P \rangle$ subgrup dari E dengan order n bilangan prima. Diberikan $\mathcal{P} = \mathbb{Z}_p^*$ di mana $\mathbb{Z}_p^* = \{\overline{a} \in \mathbb{Z}_p : \mathrm{FPB}(a, p) = 1\}$, $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^*$, didefinisikan

$$\mathcal{K} = \{(E, P, m, Q, n) : Q = mP\}$$

Nilai-nilai P, Q dan n adalah kunci publik dan $m \in \mathbb{Z}_n^*$ adalah kunci privat.
Untuk $K = (E, P, m, Q, n)$, untuk sebuah bilangan bulat acak rahasia $k \in \mathbb{Z}_n^*$, dan untuk $x \in \mathbb{Z}_p^*$, didefinisikan fungsi enkripsi

$$e_K(x, k) = (\text{Point-Compress}(kP), xx_0 \,\mathbf{mod}\, p)$$

di mana $kQ = (x_0, y_0)$ dan $x_0 \neq 0$.
Untuk *ciphertext* $y = (y_1, y_2)$, di mana $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ dan $y_2 \in \mathbb{Z}_p^*$, didefinisikan fungsi dekripsi

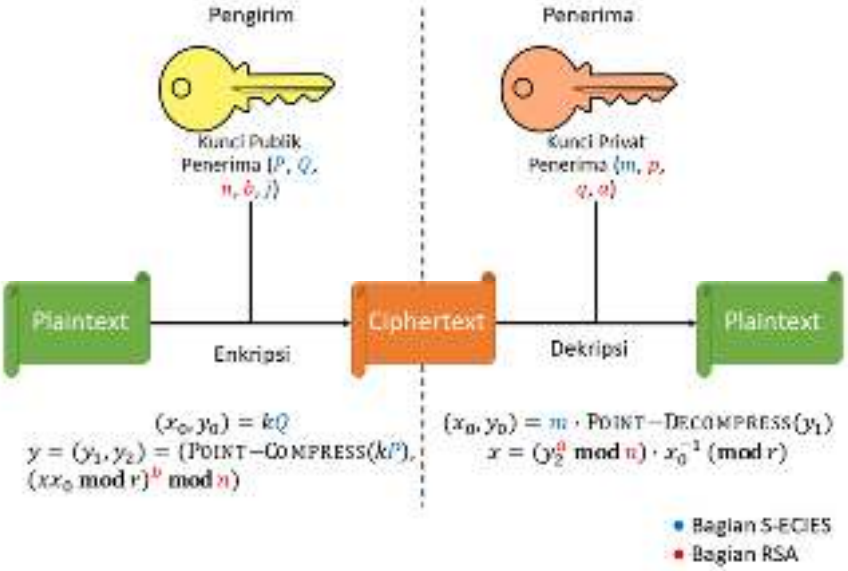
$$d_K(y) = y_2 \cdot (x_0)^{-1} \,\mathbf{mod}\, p$$

di mana

$$(x_0, y_0) = m \cdot \text{Point-Decompress}(y_1)$$

4. KRIPTOSISTEM GABUNGAN S-ECIES DAN RSA

Kriptosistem gabungan hasil dari penelitian ini adalah sebagai berikut



Gambar 4.1 Skema Kriptosistem Gabungan S-ECIES dan RSA

Algoritma kriptosistem gabungan S-ECIES dan RSA dapat dijelaskan sebagai berikut:

1. Pengirim menentukan *plaintext* yang akan dikirimkan kepada penerima. Penerima membangkitkan kunci publik dan kunci privat RSA dan S-ECIES yang akan digunakan.
2. Penerima mengirimkan kedua kunci publik kepada pengirim.
3. Pengirim melakukan enkripsi terhadap *plaintext* menggunakan kunci publik S-ECIES penerima. Hasil berupa *ciphertext* 1 yang berupa pasangan (y_1, y_s).
4. Pengirim kemudian melakukan enkripsi terhadap *ciphertext* 1 dengan cara mengenkripsi y_s menggunakan kunci publik RSA penerima menjadi y_2. Hasil berupa *ciphertext* 2 yang berupa pasangan (y_1, y_2) yang kemudian akan dikirimkan kepada penerima.
5. Penerima menerima *ciphertext* 2 dari pengirim, kemudian melakukan dekripsi terhadap y_3 menggunakan kunci privat RSA penerima. Hasil berupa *ciphertext* 1 yang berupa pasangan (y_1, y_s).
6. Penerima melakukan dekripsi terhadap *ciphertext* 1 menjadi *plaintext* menggunakan kunci privat S-ECIES penerima.

Kriptosistem gabungan ini dapat didefinisikan sebagai berikut. Diberikan E kurva eliptik pada lapangan $\mathbb{Z}_r$ ($r > 3$ bilangan prima) sedemikian sehingga terdapat $H = \langle P \rangle$ subgrup dari E dengan order j bilangan prima. Diberikan $n = pq$ dengan $n > r$, di mana p dan q merupakan bilangan prima. Diberikan $\mathcal{P} = \mathbb{Z}_r^*$ dan $\mathcal{C} = (\mathbb{Z}_r \times \mathbb{Z}_2) \times \mathbb{Z}_n$, didefinisikan:

$$\mathcal{K} = \{(n, p, q, a, b, E, P, m, Q, j) : Q = mP, ab \equiv 1 \ (\mathbf{mod}\ \phi(n))\}$$

Kunci publik dibentuk oleh P, Q, n, b dan j, dan kunci privat oleh $m \in \mathbb{Z}_j^*$, p, q dan a. Untuk $K = (n, p, q, a, b, E, P, m, Q, j)$, bilangan acak rahasia $k \in \mathbb{Z}_j^*$ dan *plaintext* $x \in \mathbb{Z}_r^*$, didefinisikan fungsi enkripsi

$$e_K(x, k) = (\text{Point-Compress}(kP), (xx_0 \ \mathbf{mod}\ r)^b \ \mathbf{mod}\ n)$$

di mana $kQ = (x_0, y_0)$ dan $x_0 \neq 0$.

Untuk *ciphertext* $y = (y_1, y_2)$ di mana $y_1 \in \mathbb{Z}_r \times \mathbb{Z}_2$ dan $y_2 \in \mathbb{Z}_n$, didefinisikan fungsi dekripsi

$$d_K(y) = (y_2^a \ \mathbf{mod}\ n) \cdot x_0^{-1} \ (\mathbf{mod}\ r)$$

di mana

$$(x_0, y_0) = m \cdot \text{Point-Decompress}(y_1)$$

a. Pembangkitan Kunci

Berikut langkah-langkah pembangkitan kunci publik dan kunci privat.

1. Pilih sebuah E kurva eliptik pada bilangan prima $\mathbb{Z}_r$ dengan $r > 127$, kemudian pilih sebuah $P \in E$ generator dari $H = \langle P \rangle \leq E$ dengan $|H| = j$ bilangan prima. Didapat nilai P, r dan j.
2. Menggunakan langkah-langkah pembangkitan kunci RSA, penerima membangkitkan nilai-nilai n, b, p, q dan a dengan syarat $n > r$.
3. Penerima membangkitkan sebuah bilangan acak $m \in \mathbb{Z}_j^*$, kemudian menghitung $Q = mP$.
4. Didapat kunci publik adalah 5-*tuple* (P, Q, n, b, j) dan kunci privat adalah 4-*tuple* (m, p, q, a).

b. Enkripsi

Langkah-langkah enkripsi adalah sebagai berikut.

1. Pengirim menentukan sebuah *plaintext* berupa teks alfanumerik. Pengirim kemudian mengubah setiap karakter pada *plaintext* menjadi bilangan bulat dengan aturan setiap karakter menjadi sebuah blok *plaintext* x_i dengan $i = 1, 2, 3, \ldots$.
2. Pengirim membangkitkan sebuah bilangan acak $k \in \mathbb{Z}_j^*$, kemudian menghitung nilai kP.
3. Pengirim kemudian melakukan kompresi titik kP. Hasil kompresi menjadi nilai y_1.

4. Pengirim kemudian menghitung nilai $(x_0, y_0) = kQ$. Pengirim kemudian menghitung nilai $y_{s_i} = x_i x_0 \ (\mathbf{mod}\ r)$ untuk setiap i.
5. Pengirim kemudian menghitung nilai $y_{2_i} = y_{s_i}^b \ (\mathbf{mod}\ n)$ dan $y_2 = \{y_{2_i}\}$.
6. Didapat *ciphertext* adalah (y_1, y_2).

c. Dekripsi

Langkah-langkah dekripsi adalah sebagai berikut.

1. Penerima menghitung nilai $(x_0, y_0) = m \cdot \text{Point-Decompress}(y_1)$.
2. Penerima kemudian menghitung nilai $y_{s_i} = y_{2_i}^a \ (\mathbf{mod}\ n)$ untuk setiap $y_{2_i} \in y_2$.
3. Penerima kemudian mendapatkan kembali blok-blok *plaintext* dengan menghitung $x_i = y_{s_i} \cdot x_0^{-1} \ (\mathbf{mod}\ r)$.
4. Penerima kemudian mengubah kembali setiap blok x_i pada *plaintext* menjadi karakter alfanumerik.

Contoh pembangkitan kunci, enkripsi dan dekripsi pada kriptosistem gabungan S-ECIES dan RSA adalah sebagai berikut: Misalkan Alice ingin mengirimkan *plaintext* berupa bilangan bulat $x = 9$. Bob kemudian memilih kurva eliptik E yang didefinisikan sebagai himpunan (x, y) yang memenuhi $y^2 = x^3 + x + 6$ pada $\mathbb{Z}_{11}$. Bob kemudian membangkit membangkitkan dua buah bilangan prima $p = 7$ dan $q = 13$, kemudian menghitung nilai $n = pq = 7 \cdot 13 = 91$ dan nilai $\phi(n) = (p-1)(q-1) = 6 \cdot 12 = 72$. Bob kemudian memilih suatu bilangan $b = 5$ yang relatif prima terhadap $\phi(n)$. Bob kemudian menghitung nilai $a = 29$ menggunakan algoritma Euclid yang diperluas.

Karena $|E| = 13$ merupakan bilangan prima, maka berdasarkan Teorema 2.2.1, E merupakan grup siklik dan seluruh titik pada E kecuali $\boldsymbol{\mathcal{O}}$ merupakan generator dari E. Bob kemudian mengambil sebuah generator $P = (2, 7) \in E$ dan sebuah bilangan bulat acak $m = 7 \in \mathbb{Z}_{13}$. Bob kemudian menghitung $Q = mP = 7(2,7) = \underbrace{P \oplus P \oplus P \oplus \ldots \oplus P}_{7} = (7, 2)$. Maka diperoleh kunci publik Bob adalah $\big((2,7), (7,2), 91, 5, 13\big)$ dan kunci privat Bob adalah (7,7,13,29). Bob kemudian mengirimkan kunci publiknya kepada Alice. Alice kemudian memilih sebuah bilangan bulat acak $k = 6 \in \mathbb{Z}_{13}$. Alice kemudian menghitung nilai $(x_0, y_0) = kQ = 6(7, 2) = (8, 3)$. Alice kemudian mengenkripsi *plaintext* menggunakan kunci publik Bob. Hasil enkripsi adalah:

$$y = (y_1, y_2) = \big(\text{Point-Compress}(kP), (xx_0 \ \mathbf{mod}\ r)^b \ \mathbf{mod}\ n\big)$$
$$= (\text{Point-Compress}\big(6(2,7)\big), (9 \cdot 8 \ \mathbf{mod}\ 11)^5 \ \mathbf{mod}\ 91)$$
$$= ((\text{Point-Compress}(7, 9), 41)$$

$= ((7,1),41)$

Alice kemudian mengirimkan *ciphertext* kepada Bob. Bob kemudian mendekripsi *ciphertext* menggunakan kunci privat Bob. Bob kemudian menghitung $(x_0, y_0) = m \cdot \text{Point-Decompress}\big((7,1)\big) = 7 \cdot (7,9) = (8,3)$. Hasil dekripsi adalah:

$$x = (y_2^a \bmod n) \cdot x_0^{-1} \pmod r$$
$$= (41^{29} \bmod 91) \cdot 8^{-1} \pmod{11}$$
$$= 9$$

Maka Bob mendapatkan pesan asli adalah $x = 9$.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa Kriptosistem gabungan S-ECIES dan RSA merupakan kriptografi kunci publik (kriptografi asimetris) yang memiliki tiga tahapan. Tahap pertama adalah pembangkitan kunci oleh penerima pesan, tahap kedua adalah enkripsi *plaintext* oleh pengirim pesan dan tahap ketiga adalah dekripsi *ciphertext* oleh penerima pesan. Kriptosistem gabungan S-ECIES dan RSA dapat mempersulit kriptanalis dalam melakukan kriptanalisis karena dibutuhkan dua algoritma dengan kompleksitas eksponensial dan sub-eksponensial untuk meretas kriptosistem ini.

REFERENSI

[1] Buchmann, J. (2004). *Introduction to Cryptography* (2nd ed.). Springer.

[2] Hankerson, D., Menezes, A., & Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography.* New York: Springer.

[3] Menezes, A., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* CRC Press.

[4] Stinson, D. (2006). *Cryptography: Theory and Practice* (3rd ed.). Boca Raton, Florida: Chapman & Hall/CRC.

[5] Susantio, D. R., & Muchtadi-Alamsyah, I. (2016). Implementation of Elliptic Curve Cryptography in Binary Field. *Journal of Physics: Conference Series, 710*, 012022. doi:10.1088/1742-6596/710/1/012022

[6] Firdaus, J., Marwati, R., Gozali, S.M., (2018). Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang ditingkatkan dan Algoritma Elgamal. Jurnal EurekaMatika, Vol. 6, No. 1, pp 23-32.